APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/596,924	06/19/2000	THOMAS A. BERSON	XER1P012	4488

7590 01/27/2005	**EXAMINER**
Patent Documentation Center	MOORTHY, ARAVIND K

ART UNIT	PAPER NUMBER
2131	

Patent Documentation Center
Xerox Corporation
100 Clinton Ave. S.
Xerox Sq. 20th Floor
Rochester, NY 14644

DATE MAILED: 01/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

		Application No.	Applicant(s)
		09/596,924	BERSON ET AL.
Office Action Summary		Examiner	Art Unit
		Aravind K Moorthy	2131

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 September 2004*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

    4a) Of the above claim(s) *22-24* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 November 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 are pending in the application.

2. Claims 1-21 stand being rejected.

3. Claims 22-24 have been cancelled.

Response to Arguments

4. Applicant's arguments filed 9/17/04 have been fully considered but they are not persuasive.

On page 7, the applicant argues that Bhagavath et al does not teach determining a price for encryption of VoIP data based on the desired privacy level. The applicant argues that Bhagavath et al does not teach step (b) of identifying a computational burden required to perform the cryptographic service. The applicant argues that the office action did not provide a citation to Bhagavath et al supporting that assertion that a computational burden was identified by Bhagavath et al.

The examiner respectfully disagrees. Bhagavath et al teaches the user having a choice of a cheaper cost by selecting the security level. The examiner asserts that the computational burden is based on the level of security that the user chooses. The examiner did provide citation for step (b) in the previous office action [column 3 line 62 to column 4 line 3].

On page 8, the applicant argues that Bhagavath et al does not teach anything about Private Information Retrieval.

The examiner respectfully disagrees. The examiner asserts that the "private information retrieval" is retrieval of media services to subscribers of the cable system.

On page 9, the applicant argues that nothing in Iwamura separately or combined with Bhagavath et al teaches a suggestion to one skilled in the art to identify a computational burden.

The examiner respectfully disagrees. The examiner asserts that Iwamura was not used to teach identifying a computational burden. As discussed above, Bhagavath et al teaches this limitation. Iwamura was used to teach a user requesting a cryptographic service specifies the privacy level and speed of performing the cryptographic service.

On page 10, the applicant argues that nothing in Billstrom separately or combined with Bhagavath et al teaches a suggestion to one skilled in the art to identify a computational burden.

The examiner respectfully disagrees. The examiner asserts that Billstrom was not used to teach identifying a computational burden. As discussed above, Bhagavath et al teaches this limitation. Billstrom was used to teach a cryptographic service that includes utilizing group authentication.

On page 11, the applicant argues that nothing in Jakobsson separately or combined with Bhagavath et al teaches a suggestion to one skilled in the art to identify a computational burden.

The examiner respectfully disagrees. The examiner asserts that Jakobsson was not used to teach identifying a computational burden. As discussed above, Bhagavath et al teaches this limitation. Jakobsson was used to teach mixed networks.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999

(AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002

do not apply when the reference is a U.S. patent resulting directly or indirectly from an

international application filed before November 29, 2000. Therefore, the prior art date of the

reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA

35 U.S.C. 102(e)).

5. **Claims 1, 2, 4, 5, 8, 9, 11, 12, 15, 16, 18 and 19 are rejected under 35 U.S.C. 102(e) as**

being anticipated by Bhagavath et al U.S. Patent No. 6,343,117 B1.

As to claims 1, 8 and 15, Bhagavath et al discloses receiving a request for a cryptographic

service [column 3, lines 54-61]. Bhagavath et al discloses identifying a computational burden

required to perform the cryptographic service, including one or more of a privacy level of the

cryptographic service or a speed of performing, the cryptographic service. Bhagavath et al

discloses determining a price of the cryptographic service based on at least one of computational

burden, privacy level, and speed [column 3 line 62 to column 4 line 3].

As to claims 2, 9, and 16, Bhagavath et al discloses that a user requesting the

cryptographic service specifies the privacy level [column 3, lines 54-63].

As to claims 4, 11 and 18, Bhagavath et al suggests requesting payment for the

cryptographic service from a user requesting the cryptographic service [column 3 line 62 to

column 4 line 3].

As to claims 5, 12 and 19, Bhagavath et al discloses that the cryptographic service

includes utilizing private information retrieval [column 3, lines 42-53].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 3, 10 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bhagavath et al U.S. Patent No. 6,343,117 B1 as applied to claims 1, 8 and 15 above, and further in view of Iwamura U.S. Patent No. 6,272,535 B1.**

As to claims 3, 10 and 17, Bhagavath et al does not teach a user requesting the cryptographic service specifies the speed of performing the cryptographic service.

Iwamura teaches that a user requesting the cryptographic service specifies the privacy level and speed of performing the cryptographic service [column 15, lines 58-66].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Bhagavath et al so that the user requesting a cryptographic service would have been able to specify the privacy level of the encryption.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Bhagavath et al by the teaching of Iwamura because different data needs a different level of privacy based on the sensitivity. So if the price of encryption were dependent on the privacy level then a user with a low priority data would want to pay less for a low level of privacy.

7. **Claims 6, 13 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bhagavath et al U.S. Patent No. 6,343,117 B1 as applied to claims 1, 8 and 15 above, and further in view of Billstrom U.S. Patent No. 5,729,537.**

As to claims 6, 13 and 20, Bhagavath et al does not teach that the cryptographic service includes utilizing group authentication.

Billstrom teaches that the cryptographic service includes utilizing group authentication [column 11, lines 22-43].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Bhagavath et al so that the cryptographic services included using group authentication.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Bhagavath et al by the teaching of Billstrom because group authentication provides anonymous access to the cryptographic service [column 5, lines 5-8].

8. **Claims 7, 14 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bhagavath et al U.S. Patent No. 6,343,117 B1 as applied to claims 1, 8 and 15 above, and further in view of Jakobsson U.S. Patent No. 6,049,613.**

As to claims 7, 14 and 21, Bhagavath et al does not teach that the cryptographic service includes utilizing mix networks.

Jakobsson teaches providing cryptographic services using mix networks [column 5, lines 7-29].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Bhagavath et al so that the cryptographic services were performed on a mix network.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Bhagavath et al by the teaching of Jakobsson because mix networks provide superior privacy, robustness, and efficiency [column 2, lines 58-60].

Conclusion

9.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
January 19, 2005

Primary Examiner